Mobile devices as stigmatizing security sensors

Gstrein, Oskar; Ritsema van Eck, Gerard

Published in:
International Data Privacy Law

DOI:
10.1093/idpl/ipx024

Publication date:
2018

MOBILE DEVICES AS STIGMATIZING SECURITY SENSORS: THE GDPR AND A FUTURE OF CROWDSOURCED 'BROKEN WINDOWS'

Oskar Josef Gstrein and Gerard Jan Ritsema van Eck

SUMMARY

- Various smartphone apps and services are available which encourage users to report where and when they feel they are in an unsafe or threatening environment.
- This user generated content may be used to build datasets, which can show areas that are considered 'bad,' and to map out 'safe' routes through such neighbourhoods.
- Despite certain advantages, this data inherently carries the danger that streets or neighbourhoods become stigmatized and already existing prejudices might be reinforced.
- Such stigmas might also result in negative consequences for property values and businesses, causing irreversible damage to certain parts of a municipality.
- Overcoming such an "evidence-based stigma" — even if based on biased, unreviewed, outdated, or inaccurate data — becomes nearly impossible and raises the question how such data should be managed.

KEYWORDS

Apps, Crowdsourcing, GDPR, Privacy, Public Space, Security.

INTRODUCTION

Nobody wants to live in a bad neighbourhood but, alas, some of us do. It is inevitable: where there are "better" neighbourhoods, there must also be neighbourhoods which are deemed to be poor, unsafe, or even dangerous. However, such perceptions can change over time: some neighbourhoods "improve" through the efforts of city councils, investors, and inhabitants; whereas others slowly become dilapidated for various reasons.

It is generally very difficult to assess the quality of a neighbourhood. Such "verdicts" are mostly based on one or several personal opinion(s). But what if socially constructed views are aggregated into datasets that are immune from the wear and tear of time? On the one hand, there could be a more accurate, evidence-based view on local conditions. On the other hand, inhabitants and local businesses could become trapped in stigmas based on datasets outside of their control. Does such data merely reflect a social situation in a public space, or does it amount to

personal data? This question merits attention as companies and local governments are starting to collect, store, analyse, and publicize such data, specifically related to feelings of fear and insecurity.

The authors of this paper aim to investigate how sets of such geo-tagged user-generated content might negatively impact neighbourhoods and the communities and individuals living within them, especially when data is misinterpreted, becomes "out-dated", inaccurate or irrelevant over time. This paper will discuss whether possible legal remedies to such problems can be found in the new European Data Protection Framework[1] which will gain binding force in the member states of the European Union (EU) in May 2018.

The authors will argue that the free development of personality needs to be taken into consideration carefully when using such data. It is necessary to observe whether effective safeguards and remedies are in place to protect individuals who are indirectly subject to such technologies. Under certain circumstances, data-based statements about a neighbourhood might easily be used or abused to describe an individual once s/he has been connected with the area concerned. In addition to individual privacy concerns, the paper also ties in to broader debates concerning the protection of privacy for groups — specifically the communities living in neighbourhoods.

This paper will make observations on this subject by investigating several websites and smartphone applications (apps) which encourage their users to report where and when they feel that they are in an insecure or threatening public space. Such crowdsourced content may be used to build datasets which can show streets and neighbourhoods that are considered 'bad.' In the following section various websites and apps in this field will be described. Then, ethical and other consequences of their use will be discussed. In the penultimate section it will be analysed whether there are legal remedies in the new EU Data Protection Framework for those who are negatively impacted by evidence based stigmas. Finally, the conclusion will provide an overview and deliver some final thoughts on ways forward.

WEBSITES AND APPS

Numerous websites and apps[2] ask users to share geotagged reports describing (inter alia) feelings of fear. The apps presented in this section have been chosen because of the diversity of actors that have initiated and supported them, and the multiplicity of purposes for which the data has been gathered. The geographical origins of each app have not been considered in the selection process, although the legal analysis in section 4 is targeted towards EU Data Pro-

1 Consisting of: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)) [2016] OJ L119/1; and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities or the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (DIR) [2016] OJ L119/89.

2 Note that the distinction between websites and apps is blurred at times: some apps function as overlays for websites, and many of the websites described are 'responsive' i.e. are easily accessible and navigable

tection law (for reasons noted there). As most of the apps are available for take-up around the globe, including in the EU, they — or apps very similar to them — could potentially influence public spaces everywhere. Because a small number of apps are discussed in some detail, the specific socio-technical affordances[3] of the apps have served as a selection criterion, rather than their geographical origins. In other words, by not limiting the examples to the EU, the authors hope to be able to provide a richer palette of examples.

The apps presented below form interesting case studies because they invite users to specifically share feelings of fear and unsafety. However, they are not the only services on which such feelings are actively being shared and from which they can thus be harvested by interested parties. Currently, there is a growing academic and industry interest in using geo-tagged posts to social media sites such as Twitter and Facebook to establish 'hot spots' where crimes might occur in the (near) future[4]. This is sometimes also referred to as an innovative form of collecting open source intelligence[5]. Williams, Burnap and Sloan even propose to consider Twitter users as "sensors" that can track criminal activities and inform law enforcement about minor public offences such as "broken windows"[6]. This usage of data from social networking sites generates largely analogous challenges to the ones discussed in this article.

Note that the purpose of this section is not to provide a definitive overview of the most popular (or even all) apps currently available in this field[7]. Furthermore, the authors cover the essential features, but do not endeavour to create a detailed analysis of each app. Finally, the authors do not intend to present any of these services as worthy or insufficient offers; nor do they recommend or not recommend their use for further development.

---

using a browser on either a smartphone or a desktop computer. Furthermore, many systems offer different functionalities on smartphones (either browser-based or in apps) than on desktop computers, but utilize the same underlying infrastructure and databases.

3 Affordances are "the perceived and actual properties of the thing, primarily those fundamental properties that determine just how the thing could possibly be used" and "provide strong clues to the operations of things." Donald A Norman, *The Design of Everyday Things* (Doubleday 1990) 9.

4 See e.g. Matthew L Williams, Pete Burnap and Luke Sloan, 'Crime Sensing with Big Data: The Affordances and Limitations of Using Open Source Communications to Estimate Crime Patterns' (2016) 57 British Journal of Criminology 320; Johannes Bendler and others, 'Investigating Crime-to-Twitter Relationships in Urban Environments—Facilitating a Virtual Neighbourhood Watch', *Proceedings of the European Conference on Information Systems (ECIS)* (2014); Matthew S Gerber, 'Predicting Crime Using Twitter and Kernel Density Estimation' (2014) 61 Decision Support Systems 115; Nick Malleson and Martin A Andresen, 'The Impact of Using Social Media Data in Crime Rate Calculations: Shifting Hot Spots and Changing Spatial Patterns' (2015) 42 Cartography and Geographic Information Science 112.

5 Kim Miller, 'How to collect Open Source Intelligence' (In Homeland Security) <http://inhomelandsecurity.com/how-to-collect-open-source-intelligence/> accessed 17 August 2017.

6 Williams (n 4) 321.

7 For an overview of apps aimed at rape prevention see Rena Bivens and Amy Adele Hasinoff, 'Rape: Is There an App for That? An Empirical Analysis of the Features of Anti-Rape Apps' [2017] Information, Communication & Society 1; For an overview of how mobile phones mediate feelings of fear in public see Kathleen M Cumiskey and Kendra Brewster, 'Mobile Phones or Pepper Spray? Imagined Mobile Intimacy as a Weapon of Self-Defense for Women' (2012) 12 Feminist Media Studies 590.

Free to Be

The "Free to be" project, which ran from October 13 to December 31 2016, collected geotagged data describing where young women in Melbourne, Australia, felt safe or unsafe. The project was initiated and paid for by Plan Australia, which is part of Plan International, an NGO most well-known for its longstanding 'Sponsor a child' programme. The company Crowdspot[8], that specializes in crowdsourcing of geospatial information, provided the app and other technical infrastructure based on OpenStreetMap data[9].

Users could add a 'happy spot' or a 'sad spot' on a map of Melbourne, and attach a description of an incident or a photograph of the area[10]. During the data collection (and for a short while afterwards) a map showing all happy and sad spots was publicly available through the app and through a web browser. Besides warning other users of places that may be "dodgy" and pointing out which routes might be safer, the collected data will also be shared with local stakeholders in the hopes of inspiring them to make changes to the physical environment[11]. Furthermore, the data is being shared with the Monash University in Melbourne in order to analyse the data[12].

My Safetipin

This project was founded with the aim of enabling vulnerable persons (especially young women) to be able to understand security risks in their neighbourhoods better, and collects data to this end. Although the app was originally only targeted at India, it is now also available in Colombia, Kenya, Indonesia, and the Philippines. The user defines circles of interests (such as the area where one lives, works, or passes through regularly). For these circles the user frequently receives updates on the security situation.

The app presents information about lighting and visibility (to determine if others can see the user when s/he crosses an area) and rates openness (to determine if the user can see around). It rates the diversity (presence of women and children), how crowded, and how close a place is to public transport. Finally, it shows the position of law enforcement agencies and allows users to share how safe they feel. Additionally, users can share their location with trusted contacts. Users can also react to submissions of others by confirming or contesting the accuracy or relevance of reports.[13]

---

8 CrowdSpot, 'Featured Projects' (*CrowdSpot*) <http://crowdspot.com.au/> accessed 22 February 2017.

9 OpenStreetMap Foundation, 'OpenStreetMap' (*OpenStreetMap*) <https://www.openstreetmap.org/> accessed 22 February 2017.

10 Lauren Day, 'Free To Be Online Map Shows Where Women Feel Unsafe in Melbourne' (*ABC News*, 8 December 2016) <http://www.abc.net.au/news/2016-12-08/free-to-be-online-map-shows-where-women-in-melbourne-feel-unsafe/8103410> accessed 3 February 2017.

11 Olivia Lambert, 'New Map Reveals Dangerous Areas for Women after Dark' (*News.Com.Au*, 27 October 2016) <http://www.news.com.au/lifestyle/real-life/news-life/new-map-reveals-dangerous-areas-for-women-after-dark/news-story/ac74124366927004dd09838cd278aba8> accessed 3 February 2017.

12 Email from Zoe Condliffe of Plan Australia to authors (8 February 2017).

13 For more info see the information on 'My Safetipin: Personal Safety' (*Google Play*, 7 April 2017) <https://play.google.com/store/apps/details?id=com.safetipin.mysafetipin> accessed 29 May 2017. The

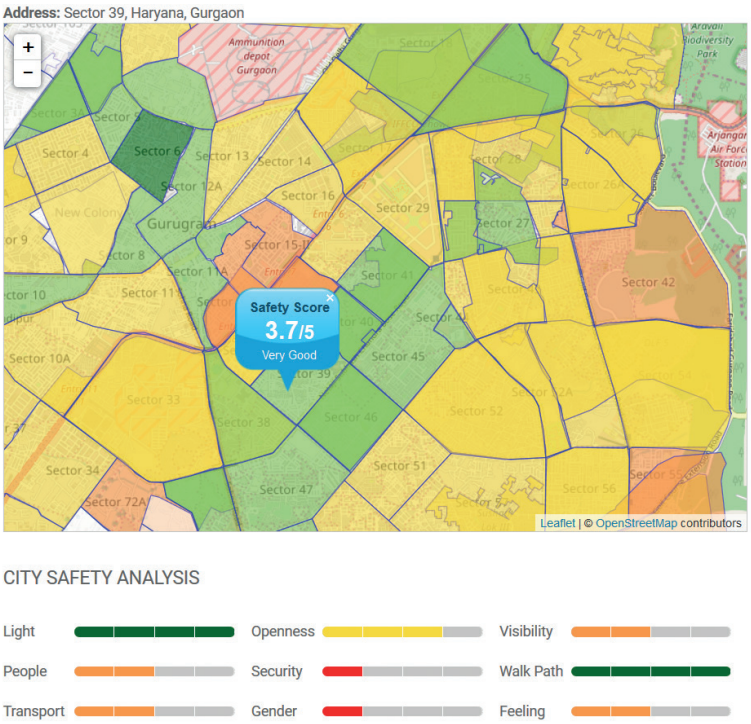

Figure 1. Screenshot by the authors of the My Safetipin website, showing the 'Safety Score' of various neighbourhoods in the Indian City of Gurgaon. In particular, Sector 39 has been selected, which allows users to see the various factors which have contributed to this particular neighbourhood's "Very Good" score. 'Safetipin' (*Apps that keep you safe*) <safetipin.com/myCiti#> accessed 22 August 2017.

Particularly interesting about this app is its attempt to shape the behaviour of both its users and policy makers. Users receive suggestions for safe walking routes, and are alerted when they enter an 'unsafe' area in order to allow them to modify their behaviour accordingly. Policy makers are targeted by putting the issue of safety (particularly safety for women when they use public transport or walk somewhere after office hours) in the public spotlight and by providing crowdsourced data to them[14].

SpotCrime & Crime Maps

SpotCrime is a predominantly USA focused website which publicizes data on crimes. The data is supplied by local law enforcement agencies, collected from news sources, and the general public can submit tips through crimetip.us[15]. It publishes this data on SpotCrime.com, where users can look up the 50 most recent crimes in a given area on a map[16] and set e-mail alerts for crimes reported in a 5 mile radius of an address. The information provided by SpotCrime is limited to the location, time, type, and sometimes a short description of the crime, and shown overlaid on Google Maps[17].

Notably, the data from SpotCrime is used by the Trulia real estate website, on which each

app is also available for iOS devices.

14 'Safetipin' (*Apps that keep you safe*) <http://safetipin.com/> accessed 29 May 2017. Aggregated data on the 'safety score' of neighbourhoods is also available through this website.

15 SpotCrime, 'Crime Tips' (*Submit a crime tip*) <https://crimetip.us/> accessed 15 February 2017.

16 Email from costumer representative "Michelle" of SpotCrime to authors (15 February 2017).

17 Google Inc., 'Google Maps' (*Google Maps*) <https://www.google.nl/maps> accessed 22 February 2017.

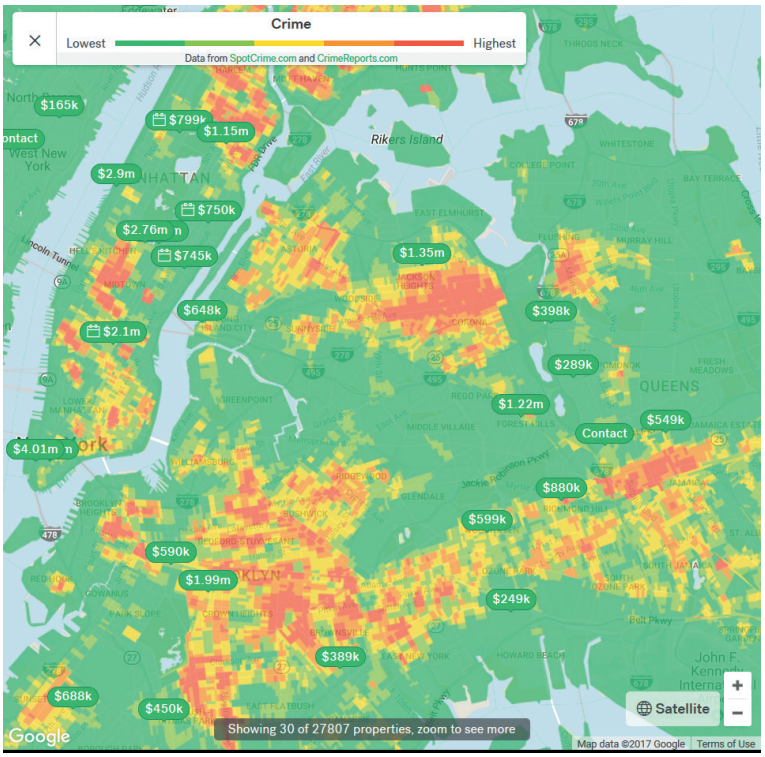

Figure 2. Screenshot by the authors of a map of Manhattan, Queens, and Brooklyn as seen on the Trulia real estate website. The map has been overlaid with crime data from SpotCrime and various 'for sale' properties. Trulia, 'Queens and Viewable map area Homes For Sale & Real Estate' (NY Real Estate & Homes for Sale) <https://www.trulia.com/for_sale/40.632112163148,40.829316775872,-74.026498761825,-73.762826886825_xy/12_zm/#map-crime> accessed 22 August 2017.

listing is accompanied by a 'Crime score' ranging from lowest to highest, which can be clicked in order to get historic data about the most recent 2500 crimes in the area[18].

A very similar app that is targeted to Brazil is Crime Maps[19]. Since most of the features mirror the ones just presented, this app will not be discussed individually.

GeoEstrela, MeldStad, and Ir-Raħal Tagħna

Various municipalities are starting to offer their citizens ways to report rubbish and damaged street furniture through mobile and desktop interfaces, usually accompanied by promises that reports will be quickly — or at least quicker than before the system was launched — dealt with. Even though such systems lie somewhat outside the focus of this paper, which is apps that can be used to report fear, they merit inclusion for at least four reasons: primarily because the harms to the reputation of a specific area are similar, although perhaps less serious; because the number of such systems seems to be growing; because the involvement of municipalities might lend the reports extra credibility; and because within community surveillance efforts aimed at increasing safety, improving the quality of life using such apps is often seen as an integral part

18 Trulia, 'Trulia Launches Crime Maps to Add Insights and More Complete Data to American Neighborhoods' (*News Room*, 2 June 2011) <http://info.trulia.com/press-releases?item=106144> accessed 14 February 2017.

19 For more information visit 'Crime Maps' (*Google Play*, 21 September 2016) <https://play.google.com/store/apps/details?id=com.rdr.mapscrimes.lite> accessed 29 May 2017.

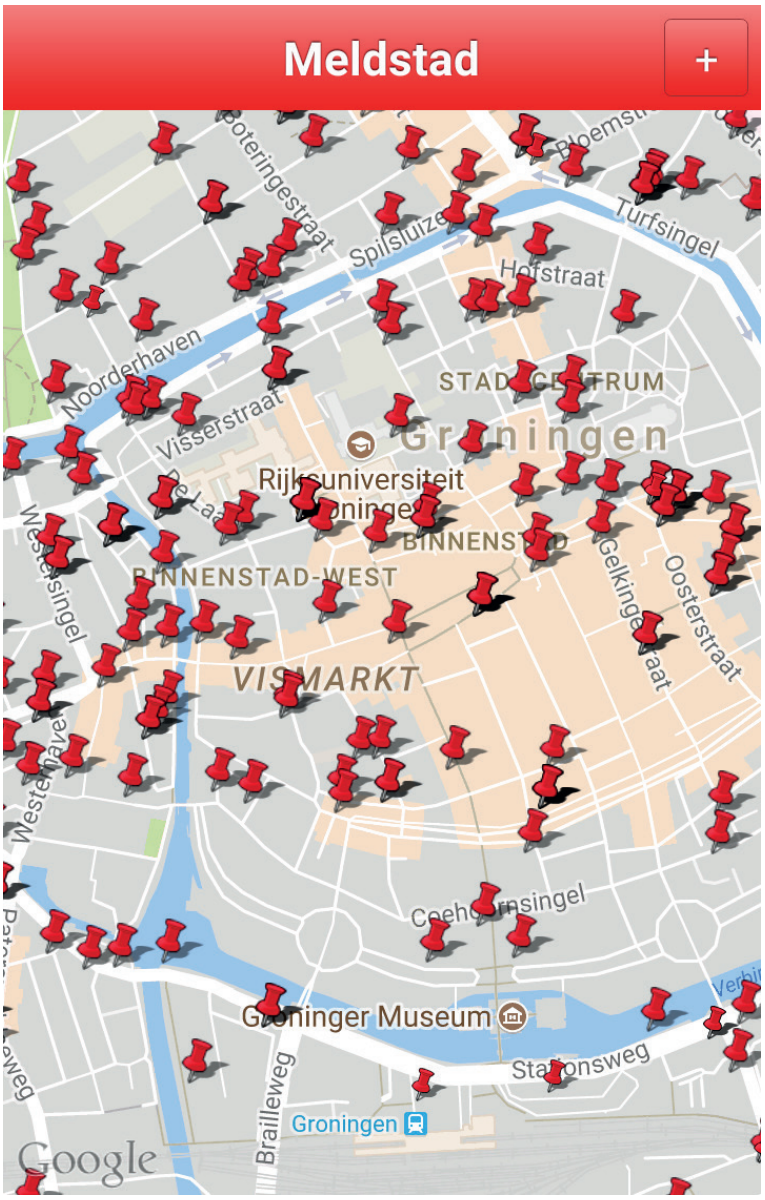

Figure 3. Screenshot taken using an Android smartphone by the authors of a map of the city centre of Groningen, The Netherlands, as seen in the Meldstad app. Outstanding reports can be seen overlaid as pushpins. Gemeente Groningen, 'Meldstad' accessed 22 August 2017.

of the program, rather than something which serves a distinct function[20].

In this subsection, three such systems will be introduced: The *GeoEstrela* system from Lisbon in Portugal, the *MeldStad* system from Groningen in the Netherlands, and the *Ir-Raħal Tagħna* system from Malta.

In the civil parish of Estrela in Lisbon of about 20,000 inhabitants, citizens can report issues such as broken street furniture, loose cobblestones, weed, faded road markings, rubbish and dog faeces through the *GeoEstrela* website[21]. The geotagged reports are shown overlaid on Google Maps on a publicly available website and stored (seemingly) indefinitely. Citizens can attach up

20 Anaïk Purenne and Grégoire Palierse, 'Towards Cities of Informers? Community-Based Surveillance in France and Canada' (2017) 15 Surveillance & Society 79, 82–5.

21 Note that there is no separate *GeoEstrela* app, but that the website is optimized for reporting when accessed using a smartphone.

to three photos to their report, and the civil parish services attaches a photo once the situation has been cleaned or repaired, which the reporting user is notified of through e-mail. The system, which was launched in late 2014, had at the time of writing received over 5,000 reports, of which more than 70% had been resolved.[22]

A similar service exists in the city of Groningen, the Netherlands: *MeldStad*, although the sort of information which can be submitted is broader: not only broken street furniture or dog faeces can be reported, but also dangerous road crossings and spots where speeding occurs regularly. Finally, requests for items such as playgrounds can also be submitted through *MeldStad*. Citizens can send their reports through a website, dedicated iOS and Android apps, or a WhatsApp number. All outstanding reports are visible on a proprietary map which is publicly available, but disappear once the report has been dealt with.[23]

A similar app which aims at improving the communication between public administration and the population has just been rolled out in the EUs smallest member state, Malta. The Ir-Raħal Tagħna (or "Our Kind of Town) app is set "to make it easier for citizens to report any problem from any spot, without the need to go personally to their respective local council."[24] At the time of writing it had been rolled out in the area of St. Paul's Bay and was available on the Google Play Store.

WayGuard

This app is available for iOS and Android. It was launched in 2016 by the German subsidiary of the insurance corporation AXA and is designed in cooperation with the local police of Cologne, Germany[25].

Once installed, a user gets the opportunity to share the current location of the device with the "WayGuard Team" and persons of trust like family members, partners, or friends. The app enables communication to persons of trust via a call or a chat function. Users can also be notified when a target, like someone's home, has been reached. Finally, should an emergency occur, an emergency call can be made easily through a dedicated function of the app. The WayGuard Team will then know the precise location of the user and notify the police.

Furthermore, the app provides information how to behave when walking or cycling to a destination or when using public transport. This content is provided in cooperation with the police of Cologne. The app has won an award for "best security app" in the year 2016 awarded

22 Junta de Freguesia da Estrela, 'GeoEstrela' (*GeoEstrela*) <https://www.jf-estrela.pt/caap/app/gso/> accessed 13 February 2017.

23 Gemeente Groningen, 'Gebreken in Uw Buurt Melden' (*Gemeente Groningen*) <https://gemeente.groningen.nl/gebreken-en-overlast-melden> accessed 13 February 2017; Gemeente Groningen, 'Meldingen Groningen' (*MeldStad*) <http://fleximap.groningen.nl/gnmaps/meldingen/> accessed 13 February 2017.

24 Nikita Kozlov as quoted in 'Our Kind of Town' (*Times of Malta*, 26 February 2017) <http://www.timesofmalta.com/articles/view/20170226/technology/Our-kind-of-town.640852> accessed 13 March 2017.

25 AXA Konzern AG, 'WayGuard: Begleit-App Für Ein Gutes Gefühl Unterwegs' (*Wayguard*, 2016) <https://www.wayguard.de/> accessed 6 February 2017.

by a German magazine[26].

POTENTIAL CONCERNS

At the start of this section it must be stated that the services presented above have different purposes, feature different designs, and are being operated in different cultural and societal circumstances. This is important to bear in mind as contextual factors such as time, space, place, economy, and technology are crucial when it comes to the fundamental human right to privacy[27].

However, there are also numerous parallel characteristics which are interesting to observe: First, all of these services have in common that they address issues of safety and fear in public spaces. Secondly, they represent innovative configurations — or: assemblages[28] — of smartphones and internet-based services. Thirdly, there is a tendency of combining several sources of data with each other to get a more complete picture of the situation in an environment, community or a neighbourhood. These sources include user inputs, news reports, law enforcement data like crime statistics, and others. Fourthly, major aspects of the assessment of a situation are based on individual perceptions of people in specific situations. Finally, most of these services are used on experimental or semi-experimental bases. None of them had become well established services with a large commercial or publicly highly relevant impact at the time of writing.

Despite the diversity of the examples presented in the previous section, their parallel characteristics mean that their usage might lead to similar, and sometimes serious, problems. We build upon the apps presented above to discuss six salient scenarios.

First, data of pseudo- or anonymous users obtained through such apps might be aggregated and combined with other records and datasets. Sometimes those might be publicly available, such as reports published by law enforcement agencies on crime statistics in the case of CrimeSpot. Potentially, non-public sources could also be used, if they are available for purchase, compromised — e.g. hacked — or available to a state authority that is legally entitled to access them even if they were originally created for other purposes. This is concerning because it cannot be guaranteed that an individual remains unidentifiable if she/he wishes to[29]. Research with med-

26 'Die Besten Apps Des Jahres 2016 – Teil 1/7' <http://androidmag.de/app-reviews/die-besten-apps-des-jahres-2016-teil-1/> accessed 27 February 2017.

27 Joseph A Cannataci, 'Report of the Special Rapporteur on the Right to Privacy' (31st Human Rights Council, 8 March 2016) para 22 <http://www.ohchr.org/Documents/Issues/Privacy/A-HRC-31-64.doc> accessed 27 February 2017; Helen Fay Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 119.

28 Kevin D Haggerty and Richard V Ericson, 'The Surveillant Assemblage' (2000) 51 British Journal of Sociology 605.

29 In order to present a clearer conclusion on the state of arts in this area the UN Special Rapporteur on the right to Privacy, Joseph A. Cannataci, intends to work on a Thematic Action Stream entitled "Big Data and Open Data". For more information see Joseph A Cannataci, 'Parallel Streams of Action (TAS) for the Mandate of the UN Special Rapporteur for Privacy and the First Set of Priorities' <https://www.privacyandpersonality.org/2016/06/privacy-and-personality-blog-3-parallel-streams-of-action-tas-for-the-mandate-of-the-un-special-rapporteur-for-privacy-and-the-first-set-of-priorities/> accessed 8 March 2017.

ical records and studies with credit card information have shown that it is surprisingly easy to single out individuals from large, seemingly pseudonymized or anonymized sets of data[30].

Additionally, there seems to be significant interest and resources to improve data analytic techniques. Hence, it might be the case that a method for pseudo- or anonymization works for the moment, but not in the future. This is very worrying for users who report feeling vulnerable and at risk of victimization.

As will be discussed in the legal analysis in more detail, the new EU Data Protection Framework provides safeguards for data once it qualifies as "personal" in line with the legal definition. However, what seems concerning are those instances in which data that doesn't fit the legal definition of personal data does allow for the extraction of general behavioural patterns or conclusions regarding situational circumstances once it is combined with data from other sources. Although data analytic techniques marketed as "big data", "open data", "artificial intelligence" and "deep learning" are rapidly evolving to make this ever easier, the legal frameworks largely fail to address these potential concerns.

This is particularly worrisome if decisions are based on the combination of data sources in the absence of societal experience or legitimate knowledge on how to combine such sources to actually predict human behaviour[31]. The discussion on implicit or "baked-in" discrimination when employing smart or autonomous decision making is currently just beginning to take shape on a broad interdisciplinary level[32] and will be discussed further below. Nevertheless, there seems to be an overwhelming economical and political desire to roll out these technologies on an unprecedented scale as fast as possible in order to reap the economic gains.

Secondly, any technology we use makes us increasingly traceable by state or corporate

30 For the medical sector see the work of Latanya Sweeney. For example 'Only You, Your Doctor, and Many Others May Know' [2015] Technology Science <http://techscience.org/ a/2015092903>. For the study on credit card data see Yves-Alexandre de Montjoye and others, 'Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata' (2015) 347 Science 536.

31 This problem has also been discussed in connection with the use of proprietary software ("COMPAS") in the United States of America. In order to help judges make decisions on probation conditions of individuals the software suggested a probability score which should reflect how likely a person would commit another crime in the future. After a critical investigation of the results of the software there were claims that it discriminates against black defendants. The claim was denied by the development company. The score was based on a questionnaire which did not include questions on race, but there was also not sufficient testing if the questions would result in biased scores. More discussion can be found at Julia Angwin et al, 'Machine Bias' <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 17 August 2017; Oskar Josef Gstrein, 'How to approach technology, human rights and personality in the digital age? – A few thoughts' <https://www.privacyandpersonality.org/2016/10/how-to-approach-technology-human-rights-and-personality-in-the-digital-age-a-few-thoughts/ > accessed 17 August 2017.

32 In Germany for example, a Civil Society Organisation with the title "Algorithm Watch" has been founded recently. To read more about the initiative see Matthias Spielkamp, 'Inspecting algorithms for bias' (*MIT Technology Review*, 12 June 2017) < https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias/> accessed 18 August 2017. In the United States the "AI NOW initiative" strives to contribute to develop a better understanding of the social impacts of Artificial Intelligence. It also issues annual reports with recommendations <https://artificialintelligencenow.com/> accessed 18 August 2017. One of the authors of this paper has presented on the issue at a Special Workshop of IVR 2017 World Congress in Lisbon entitled "New Technology and (Non-)Human Agency: Risks, Responsibilities and Regulation".

actors through the burgeoning surveillant assemblage operating in public spaces, especially in areas saturated with high-tech infrastructure[33]. This decreases the options for staying private in public both quantitatively — the amount of public spaces in which privacy is possible decreases — and qualitatively — the amount of privacy possible in public spaces decreases. Easily accessible spaces of privacy where personal development is possible under less societal restraints are essential[34], as is the availability of a modicum of privacy in public[35].

However, this seems currently threatened more than ever due to technological and societal developments[36]. Most people carry electronic sensors permanently in their pockets or on their wrists in the forms of smartphones, -watches, or other wearables which can track their wearers and those around them[37]. This creates environments in which surveillance is so ubiquitous as to become ambient[38]. This leads to an hollowed out expectation of privacy in public[39]. The apps under scrutiny form an especially interesting category of artefacts, as they encourage citizens to actively use these sensors and upload data on safety and fear. This raises the stakes for anyone captured in the shared (meta-)[40].

This phenomenon could be referred to as "technological gentrification". Similar to areas in communities which see a steep rise in rents and real estate prices because there is a rapid growth in investment capital, ubiquitously deployed surveillance infrastructure deprives the large majority of individuals of the opportunity to develop freely and equally. Hence, community areas which are "technologically gentrified" will solidify social structures up to a level where the potential of individual and collective development will be drastically reduced.

Finally, the re-identification, already pointed to above, of either the user of the app or others might in turn also facilitate further tracking, behavioural profiling, and monitoring[41].

---

33 See for citizens' perspectives and scenarios Linnet Taylor and others, 'Customers, Users or Citizens? Inclusion, Spatial Data and Governance in the Smart City' (Maps4Society Final Project Report 2016) <http://ssrn.com/abstract=2792565> accessed 23 March 2017.

34 Danah Boyd and Alice E Marwick, 'Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies', *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society* (2011) http://papers.ssrn.com/sol3/papers.cfm? abstract_id=1925128; Julie E Cohen, 'What Privacy Is for' (2013) 126 Harvard Law Review 1904.

35 Nissenbaum (n 27) 139; Alan F Westin, *Privacy and Freedom* (The Bodly Head 1967) 35.

36 See the upcoming volume edited by Bert-Jaap Koops, Tjerk Timan and Bruce Clayton Newell, *Surveillance, Privacy, and Public Space* (Routledge) and Marja Beckers, 'Absender Unbekannt' [2017] Hohe Luft 54.

37 Ivo Flammer, 'Genteel Wearables: Bystander-Centered Design' (2016) 14 IEEE Security & Privacy 73.

38 For a similar argument in the online world, see Joel R Reidenberg, 'The Transparent Citizen' (2015) 47 Loyola University Chicago Law Journal 437.

39 Joel R Reidenberg, 'Privacy in Public' (2014) 69 University of Miami Law Review 141.

40 Gerard Jan Ritsema van Eck, 'Emergency Calls with a Photo Attached: The Effects of Urging Citizens to use their Smartphones for Surveillance' in Bert-Jaap Koops, Tjerk Timan and Bruce Clayton Newell (eds), *Surveillance, Privacy, and Public Space* (Routledge) (forthcoming).

41 Online tracking might be associated mainly with cookies and IP-addresses. However, it is also possible to use other methods such as the combination of certain characteristics of a device (operating system, screen resolution, web browser and version number, etc.). Steven Englehardt and Arvind Narayanan, 'Online Tracking: A 1-Million-Site Measurement and Analysis' (2016) <http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf> accessed 23 March 2017. For a (currently

Thirdly, a potential concern in the use of such technologies is how they might lead to prejudices against communities by presenting (aggregated) individual feelings or sentiments. Although this makes them seem "evidence-based," they are based on incomplete and biased datasets. There is the danger that the sample of users of an app like "WayGuard", for example, is too small to be used as a basis for a verdict. Furthermore, not only the amount of data might be concerning, but also the portion of society (e.g. mostly young, female or male, tech-savvy etc.) which contributes to the dataset might be concerning[42]. Ultimately, there is the issue of discrimination in the data collection: When prodded to watch for suspicious behaviour, people disproportionally rely on stereotypes[43] to decide who and what is "out of the ordinary;" which is decidedly different than the legally prescribed category of suspicion[44]. Thus, areas with more young, black males[45] might receive more negative reviews than warranted. Also note here that low-income and ethnically diverse neighbourhoods tend to participate less in online platforms like GeoEstrela, thus skewing the data even further[46]. The picture which emerges from crowd-generated content is thus not an objective photograph, but rather an impressionistic painting[47].

In general, it is questionable if subjective feelings should serve as a basis to come to a verdict about (parts of) communities. The neighbourhood that one person finds inspiring and important, sometimes is unsafe and unsound for another. In that context, it might be interesting to remember that quarters like Montmartre in Paris or Friedrichshain in Berlin, which are "established" or "hip" at the moment, have both had a reputation for being less fancy and at times very unsafe. With the passing of time both of them have managed to increase their reputation and became quarters which are sought after and even famous. Hence, the question arises whether it is favourable to collect and disseminate data which marks areas for being very dangerous or unsafe. Can such stigmas still be overcome if they are backed up by widely available data[48]?

Fourthly, there is the issue of repurposing of data. Data created by such services may be

patched) example of how aspects that one might not consider can make one traceable see Lukasz Olejnik and others, 'The Leaking Battery: A Privacy Analysis of the HTML5 Battery Status API' [2015] International Association for Cryptologic Research (e-Print archive) <https://eprint.iacr.org/2015/616.pdf> accessed 22 February 2017.

42 For a broader discussion and empirical example on the basis of twitter usage in NYC, see Luc Anselin and Sarah Williams, 'Digital Neighborhoods' (2016) 9 Journal of Urbanism: International Research on Placemaking and Urban Sustainability 305.

43 Clive Norris and Gary Armstrong, 'CCTV and the Social Structuring of Surveillance' (1999) 10 Crime Prevention Studies 157.

44 Sebastian Larsson, 'A First Line of Defence? Vigilant Surveillance, Participatory Policing, and the Reporting of "Suspicious" Activity' (2017) 15 Surveillance & Society 94.

45 Norris and Armstrong (n 43) 162–3.

46 Burak Pak, Alvin Chua and Andrew Vande Moere, 'FixMyStreet Brussels: Socio-Demographic Inequality in Crowdsourced Civic Participation' [2017] Journal of Urban Technology 1.

47 AT Crooks and others, 'User-Generated Big Data and Urban Morphology' (2016) 42 Built Environment 396, 411.

48 Henri Lefebvre, *The Production of Space* (Donald Nicholson-Smith tr, Blackwell 1991), especially page 165 thereof.

sold or resold by corporations and become subject to business models that can lead to negative and potentially illegitimate effects affecting the dignity of persons living or working in any area covered by the app in question. Less dramatic might be repurposing of the data that is in line with the legal framework, but still questionable.

Concerned individuals are often unaware of the practices and existence of data brokers which sell or re-sell data to support marketing efforts, mitigate risks, or facilitate the search for people[49]. One example that is frequently reported is credit scoring, which is sometimes heavily based on the postal code a person is registered under[50]. In the United States of America, where this type of business is very developed, some authors call for legislative measures which increase transparency and accountability. The ultimate goal is to give individuals — who are typically consumers — more control over data which relates to them[51]. In Europe the Commission of the EU has set new initiatives at the beginning of 2017 to assess the impact and potential of commercial exploitation of non-personal data which is not covered by the new Data Protection Framework. These "next steps towards a European data economy" include an assessment of the activities of data brokers[52]. Both of these initiatives remain nationally or regionally limited and tied to economic regulation.

The question remains what happens when some of this data is traded or transferred across global regions. Transborder data flows regulation should generally be considered from a perspective of legal pluralism[53]. However, the lack of a specific legally binding international framework for the sale and re-sale of data makes it likely that regional and international human rights frameworks will remain the starting points to address concerns arising from cross-regional transfer or commercial exploitation of such data.

Efforts to build cross-regional bridges based on mutual legal assistance and reciprocity, such as the EU-US "Safe Harbour" or "Privacy Shield" regime, have their difficulties in withstanding the temptations of extraterritorial application of specific laws of the respective partners[54].

---

49 Stephen Beake, 'Data Brokers and the Need for Transparency and accountability' (Nova Science Publishers 2014) 29.

50 This is a problem in connection with the larger issue of trading personal data; Barbara Wimmer, 'Adresshandel: Das Geschäft Mit Unseren Persönlichen Daten' (*futurezone*, 12 January 2015). <https://futurezone.at/netzpolitik/adresshandel-das-geschaeft-mit-unseren-persoenlichen-daten/100.371.363> accessed 27 February 2017.

51 Beake (n 49) 56.

52 European Commission, 'Commission outlines next steps towards a European data economy' (2017) IP/17/5.

53 Christopher Kuner, 'Transborder data flows and data privacy law' (Oxford University Press 2013) 164, 166.

54 The EU-US Safe Harbour regime (Decision 2000/520/EC) was declared void by a judgment of the CJEU in case C–362/14 *Maximillian Schrems v Data Protection Commissioner* EU:C:2015:650. It was then replaced with the Privacy Shield ((EU) 2016/1250). However, there remains severe scepticism on the European level whether Privacy Shield lives up to its promises. The influential Art 29 Working Group has issued a statement on 13 June 2017 in which it requests more evidence that the guarantees are actually kept <http://ec.europa.eu/newsroom/document.cfm?doc_id=45272> accessed 18 August 2017. Some courts in the US require international corporations such as Google to hand-over personal data to US authorities regardless where they are stored, see e.g. *Google Inc*, ND Cal, No 16-mc-08263, review

Hence, it remains to be seen how much needed international standards and rules will evolve.

Additionally, if data remains in the public domain for an indefinite amount of time it is questionable how it will be used by different governmental actors. This is becoming increasingly topical considering the vast amount of data created for various purposes. There exist drastic historic examples of how this had negative effects for certain parts of societies in the past[55].

For example, the Netherlands had a very comprehensive population registration system before they were invaded by Nazi Germany in 1939. After the regime change, the specific and precise data was abused to enable many Jewish deaths[56]. Looking at the kind of data being gathered by apps such as those described in the previous section, one could imagine it being used to justify repressive policies against certain neighbourhoods and the communities living in them[57].

Fifthly, there might be various financial harms. Real estate owners might be facing decreasing property values if potential buyers are scared away by high levels of reported fear in certain areas. Trullia, the second most popular real estate website in the USA[58], already provides such a score for each property listed based on SpotCrime data. Furthermore, shops and other businesses operating in a certain area might face a slinking away of their patronage.

A sixth point of concern emerges if besides potential homebuyers, law enforcement agencies also start using user generated data to inform their decisions and deploy resources. It is easily imaginable that "predictive policing" — which has law enforcement agencies using software to simulate the needs of a community for policing and which uses factors like past crime statistics, weather predictions, etc. — might also include the data from services like WayGuard[59].

In a positive light, this could be seen as responding to citizens' needs. However, there might also be downsides. First of all, such patrolling might create a self-fulfilling prophecy: there will be more arrests in areas with a higher police presence[60], which consequently justifies the negative reports and increased surveillance[61], which in turn further damages the reputation of a

---

denied 8/14/17. See also Daniel R. Stoller, 'Google Must Turn Over Data Stored Abroad Sought Under U.S. Warrant' (Bloomberg, 15 August 2017) <https://www.bna.com/google-turn-data-n73014463160/ > accessed 18 August 2017. While Google will most likely attempt to bring this issue in front of the US Supreme Court it is not unlikely that similar decisions will be made by courts in the future. Such actions — on both sides — threaten the basic consent of the parties which lead to the original agreement. Hence, it seems only a question of time until the Privacy Shield will collapse in a manner similar to Safe Harbour.

55 William Seltzer and Margo Anderson, 'The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses' (2001) 68 Social Research 481.

56 Ibidem, p. 486–488.

57 For a poignant example of how repressive regimes can present poor neighbourhoods and the communities living in them as creating societal injustices, rather than being the result of them, see Mustafa Dikeç, 'Police, Politics, and the Right to the City' (2002) 58 GeoJournal 91.

58 'Top Sites by Category: Regional/North America/United States/Business and Economy/Real Estate' (*Alexa*) <http://www.alexa.com/topsites/category/Regional/North_America/United_States/Business_and_Economy/Real_Estate> accessed 29 March 2017.

59 See e.g. 'How PredPol Works: We Provide Guidance on Where and When to Patrol' (*PredPol*, 2015) <http://www.predpol.com/how-predpol-works/> accessed 9 May 2016.

60 For a similar argument in the data of big context analytics, see Elizabeth E Joh, 'Policing by Numbers: Big Data and the Fourth Amendment' (2014) 89 Washington Law Review 35.

61 Julia van Heek, Katrin Arning and Martina Ziefle, '"How Fear of Crime Affects Needs for Privacy &

certain area without targeting the root causes of crime[62]. However, even if no arrests are made, increased police surveillance can by itself already inhibit free expression, movement and unconventional behaviour, especially in already marginalized communities with strained relations to law enforcement agencies[63]. We will not come back to this point as a European framework with regards to the use of police data for predictive policing is currently lacking[64]. However, the need for a public debate and awareness of the use of such data seems evident.

LEGAL ANALYSIS

After flagging some concerns regarding the apps and services the authors presented in the previous section, this section will aim at providing a legal analysis of the situation. However, this cannot be done without putting such an effort in context.

As a reference framework, the revised European Union Data Protection Framework[65] will be used, which is about to become legally binding in May 2018. The choice of this framework is useful because the situation in Europe will be more strongly harmonized than at the time of writing of this document. This will result in a situation with less national differences in regulation between European countries. Additionally, at its core this text is an international text which seems useful when considering potential general problems arising from the use of apps which relate to security and fear. Furthermore, the new legal texts might be considered as benchmarks when it comes to the achievements of legislative activity in the area which might also be interesting for other regions of the global community[66]. Another formal argument for

Safety" - Acceptance of Surveillance Technologies in Smart Cities' in Cornel Klein, Brian Donnellan and Markus Helfert (eds), *Proceedings of the 5th International Conference on Smart Cities and Green ICT Systems* (Science and Technology Publications 2016) 40–1.

62 Taylor Shelton, 'The Urban Geographical Imagination in the Age of Big Data' (2017) 4 Big Data & Society 1, 3–7; Peter Mantello, 'The Machine That Ate Bad People: The Ontopolitics of the Precrime Assemblage' (2016) 3 Big Data & Society 1, 6; Edward W Soja, 'The Socia-Spatial Dialectic' (1980) 70 Annals of the Association of American Geographers 207.

63 Elizabeth E Joh, 'The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing' (2016) 10 Harvard Law & Policy Review 15, 31–2; Alessandro Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection' (2016) 32 Computer Law & Security Review 238, 240.

64 Francesca Bosco and others have detailed, as an example of the lack of harmonization, the opaque framework of 'hardly comprehensible' rules regulating the myriad German police databases. 'Profiling Technologies and Fundamental Rights and Values: Regulatory Challenges and Perspectives from European Data Protection Authorities' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Reforming European Data Protection Law* (Springer 2015) 14–15. The courts in both Luxembourg and Strasbourg have not had ample opportunity yet to develop case law on the subject, see Rosamunde van Brakel and Paul de Hert, 'Policing, Surveillance and Law in a Pre-Crime Society: Understanding the Consequences of Technology Based Strategies' [2011] Cahiers Politiestudies 163, 185. The closest to a legal framework comes the non-binding Council of Europe Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to the automatic processing of personal data in the context of profiling <https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016805cdd00> accessed 11 Augustus 2017.

65 See footnote 1.

66 European Commission, 'Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection' <http://europa.eu/rapid/press-release_STATEMENT-16-1403_en.htm> accessed 24 March 2017.

choosing the European Union Data Protection Framework as a reference framework is Article 3 of the GDPR, which results in an exceptionally broad territorial scope. According to Article 3 par. 2 lit. b a controller or processor of personal data is subject to the regulation if it is operating outside of the EU, but the handling of personal data relates to a data subject whose behaviour takes place within the Union. Ultimately, since the texts of GDPR and DIR have been adopted recently in April 2016[67], one would hope that the issues presented by the current state of technological development are addressed entirely or at least sufficiently.

Because the data gathered by the operators of the apps and services can be used by private and public authorities (particularly law enforcement agencies; LEAs) the General Data Protection Regulation (GDPR) and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (DIR) will be considered. However, before going into specific legislation, it is useful to look at the bigger legal picture.

Personal Data as "Resource"?

In order to motivate her nation to be more dynamic in the area and leave the old paradigm of "purpose limitation" behind, German Chancellor, Angela Merkel, has been referring to data as "the resource of the 21st century"[68]. Indeed, corporations like Alphabet Inc., the parent company of Google, Facebook and others[69] have created economic imperia based on the creation, storage, analysis, and commercialization of personal data[70]. Furthermore, public administrations are under increasing pressure to become more cost effective, efficient, and responsive. One of the possible strategies to achieve this is the automation and standardisation of internal and external communication. In short: the private and public sector are increasingly using automated personal data processing to improve their performance.

This raises challenges for the fundamental human rights framework developed to safeguard privacy and the use of personal data. This framework traditionally addresses primarily the state and its authorities[71], However, both the general framework and privacy in particular have changed significantly over time and with the transition to the digital age[72]. While "being left

67 Ibidem; GDPR Art. 99; DIR Art. 65.

68 'Merkel: Daten Sind Rohstoffe Des 21. Jahrhunderts' (*heise online*, 2 November 2015) <http://www.heise.de/newsticker/ meldung/Merkel-Daten-sind-Rohstoffe-des-21-Jahrhunderts-2867735.html> accessed 6 March 2017.

69 'G Is for Google' (*Alphabet*) <https://abc.xyz/> accessed 6 March 2017; 'Facebook – Log In or Sign Up' (*Facebook)* <https://www.facebook.com> accessed 22 August 2017.

70 'The World's Most Valuable Resource Is No Longer Oil, but Data' (*The Economist*, 6 May 2017) <http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource> accessed 29 May 2017.

71 This is based on the fact that states were the first ones with the interest and ability to process large amounts of personal data for administrative purposes. See for instance Bart van der Sloot, 'Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation' (2014) 4 International Data Privacy Law 307.

72 Remember the introduction to the famous article of Warren and Brandeis on the right to privacy in this context. Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193, 193–196.

alone" can be linked to a "liberal" or first-generational human rights tradition which emphasizes the protection of the individual with inalienable rights against the threats posed by state authorities not controlled by the rule of law, rights concern the composition of society [73]. In other words: The question is no longer only how to protect an individual from an illegitimate (historically physical) interference by a state, but now also compromises of spheres of personal autonomy (closer to the German tradition of "informational self-determination") and the regulation of access to those spheres of personal development by the State and other members of society such as corporations[74].

For reasons of enforcement and sovereignty concerns, the human rights framework still emphasizes the obligations of the state towards the people living on its territory and largely sticks to the first-generation pattern. Additionally, an obligation is added for the State to create an environment which respects and promotes rights such as privacy which transforms privacy from a "right to be let alone" to a second-generational "social right". At this stage, regulation of private corporations by states and regional bodies (which draw their legitimacy from states who pass their sovereignty onto them in specific areas) such as the EU come into play. The activities of corporations that affect large groups of people are mostly addressed in laws referring to (or "protecting") consumers. All other relationships are, from a legal perspective, subject to private law and contractual freedom. The latter comes with the assumption that parties have more or less equal power and tools at their disposal to defend their interests.

However, the use of data as a "resource" challenges this setup significantly and provokes the question whether the current legal system is able to adequately address the challenges of the digital age. Specifically, the apps and services described in this article partly pose questions which resemble situations in which "collective rights" or third-generational human rights concerns appear.

Often individual users and small businesses face much bigger corporations when personal data has been captured, and this is no different if the data capture has taken place in a public space as a result of an action by another user or ambient sensor[75]. Many corporations operate internationally and are thus hard to regulate for individual states. It is questionable if their tools and methods are as powerful as the ones of their counterparts, which is the assumption that the legal order is based on[76].

---

73 The division of human rights into three generations goes back to the end of the 1970s and is accredited to Karel Vasak who resorts to liberal or "negative" rights, "social" rights, and "rights of solidarity". Karel Vasak, 'A 30-year struggle' (1977) UNESCO Courier 30, 29.

74 This idea still dates back to the famous census judgment of the German Federal Constitutional court from 15 December 1983.The judgment itself is focused on the actions of state authorities and not private parties. German Federal Constitutional Court, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

75 Lilian Edwards, 'Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective' (2016) 2 European Data Protection Law Review 28, 38–9.

76 Lisa M Austin, 'Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)' in Austin Sarat (ed), *A World Without Privacy: What Law Can and Should Do?* (Cambridge University Press 2015) 161; Alessandro Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds),

The only common denominator to protect humans from the negative consequences of data processing is thus dignity, or human rights in legal terms. However, it remains disputed to which these are binding for large, international corporations such as the ones who collect and process the lion's share of personal data in the digital age.

Recently there is a tendency within the United Nations to place more responsibility on large technological corporations, which includes the responsibility to act as promotor and guardians of human rights like privacy[77]. However, states themselves remain primarily responsible for the protection of such rights and the creation of an environment which is beneficial for human rights[78]. One crucial aspect in that regard, is to guarantee human rights regardless of whether a person is a citizen of a specific country or not[79].

Re-identification through Combination

Fundamental Human Rights are not only protected in constitutions or documents like the Charter of Fundamental Rights of the European Union[80] (CFEU). They are also — and with greater precision — enshrined in acts based on them, such as the GDPR, which covers the handling of private data by corporations, and the DIR, which focuses on personal data that is used for purposes to ensure public security by competent authorities[81].

When considering their applicability, however, one must keep in mind the exceptions of their material scope: Anything which falls outside the general scope of EU law is not covered, as well as anything within the scope of the specific provisions on the common foreign and security policy of the EU, and personal data processed in the context of household uses[82].

Further limiting their applicability is the seemingly uncontroversial definition of 'personal data' in both the GDPR[83] and the DIR[84], which both state identically: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier

Group Privacy: New Challenges of data technologies (Springer 2017) 149.

77 UNCHR, 'The right to privacy in the digital age' UN Doc A/HRC/34/L.7/Rev.1,3: "Recalling that business enterprises have a responsibility to respect human rights as set out in the Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, and that the obligation and the primary responsibility to promote and protect human rights and fundamental freedoms lie with the State […]."

78 Ibidem.

79 UNCHR 'Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci' UN Doc A/HRC/34/60, para 44: "WHO deserves the right to privacy = everybody, everywhere. RECOMMENDATION: States should prepare themselves to ensure that both domestically and internationally, Privacy be respected as a truly universal right – and, especially when it comes to surveillance carried out on the Internet, privacy should not be a right that depends on the passport in your pocket."

80 Charter of Fundamental Rights of the European Union [2016] OJ C202/389.

81 DIR Art. 1 par. 2 lit. a; GDPR Art. 1 par. 2.

82 GDPR Art. 2 par. 2.

83 GDPR Art. 4 par. 1.

84 DIR Art. 3 par.1.

or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

This definition seems comprehensive at first glance. However, it is not helpful when resolving an old dogmatic conflict between legal scholars about the meaning of "personal" in the combination "personal data."[85] There is an abstract theory (or 'objective criterion') which says that personal data is data that can be tied to a person in view of all the knowledge that exists about it, regardless of the circumstances or the situation or the actors handling it (in legal terms the processor or controller). The concrete theory (or 'relative criterion') however, focuses on the specific knowledge and means a processor or controller of the data has and only considers data to be personal if an actor is able to tie data to a person in the known circumstances. The difference is that under the abstract theory more data has to be protected and less data is exploitable for economical or other causes[86].

The definition of personal data in the EU does not clearly indicate whether it is based on the abstract or concrete theory. As already referred to above, the GDPR[87] and the DIR[88] both refer identically to "an identifiable natural person (…) who can be identified, directly or indirectly (…)." Recently, in the case of *Breyer v Germany* on the question of whether dynamic IP addresses are personal data, the CJEU appeared to suggest that it is developing a tendency towards the abstract theory[89]. It held that (dynamic) Internet Protocol addresses collected by the German government to prevent attacks on governmental websites constitute personal data, because the users of those addresses could be identified with the help of Internet Service Providers[90]. This could suggest that the CJEU has finally acknowledged that the abstract theory has prevailed.

However, on closer scrutiny, the arguments of the judges reveal that this decision can hardly be generalized. The court itself opens several venues to the legality of such a collection of data: if consent of the user was sought[91]; if legal safeguards would be introduced which prohibit the identification process; and — most saliently for the abstract/concrete discussion — if the requirements in time, cost, and manpower would be so disproportionate "that the risk of identification appears in reality to be insignificant"[92]. Hence, it is submitted that it is not possible to

85 This conflict seems particularly present in the legal discourse in Germany ("relative oder absolute Bestimmbarkeit"). Judith Nink, Jan Pole, 'Die Bestimmbarkeit des Personenbezugs - Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze' (2015) Multimedia und Recht 563; Matthias Bergt, 'Die Bestimmbarkeit als Grundproblem des Datenschutzrechts - Überblick über den Theorienstreit und Lösungsvorschlag' (2015) Zeitschrift für Datenschutz 365; Wolfgang Ziebarth, 'Perspektive der Bestimmbarkeit' in Sydow Gernot (ed), *Europäische Datenschutzgrundverordnung* (Nomos 2017) DSGVO Art. 4 Rn. 33-40. See also para 25 of Case C–582/14 *Patrick Breyer v Bundesrepublik Deutschland* EU:C:2016:779, in which the CJEU mentions this conflict.

86 See Case C–582/14 *Patrick Breyer v Bundesrepublik Deutschland* EU:C:2016:779, para 25.

87 GDPR Art. 4 par. 1.

88 DIR Art. 3 par. 1.

89 Case C–582/14 *Patrick Breyer v Bundesrepublik Deutschland* ECLI:EU:C:2016:779.

90 Ibidem, para 49.

91 Ibidem, para 64. The whole second question in the judgement revolves around the subject of consent or the lack thereof.

92 Ibidem, para 45-49.

interpret this judgment as a categorical decision by the CJEU to stick to either the abstract or the concrete theory. In effect, the judgement only adds one more nuance to this complex problem.

Think about this distinction in the light of the considerations raised in the above section: although it might not be possible to tie certain specific data points to a person by using just one database, it might become possible by combining one (maybe closed) database with other (maybe openly available) databases. For example, the data gathered by an app like My Safetipin might not be considered personal data per se in legal terms, but combined with other databases (such as open street maps, newspaper articles, police reports, etc.) it might be possible to identify some users of the app.

This raises the question if a potential gap in the definition exists that appears when the combination of two (or more) datasets that don't contain personal data actually produces personal data. The safeguards enshrined in the DIR and GDPR which prohibit the reuse of data for incompatible purposes don't apply to indirectly personally identifiable data as presented above[93], and consider each source of data on a case by case basis.

Potential Remedies on the Basis of the New EU Legislation

Generally, protection of the law can exist for legal persons, such as corporations, foundations, or public authorities, and natural persons. Focusing first on legal persons, their ability to have their interests covered by fundamental rights is limited and varies from country to country, even within the EU[94]. This means, for example, that entrepreneurs who run businesses in areas which are perceived to be prone to crimes like robbery and murder according to services like SpotCrime are not entitled to remedies under either the GDPR or the DIR[95].

The CFEU might entitle the owners of businesses or assets like apartments or houses to some sort of remedy if they can prove that their right to property in Art. 17 is being infringed in a personal capacity. However, par. 1 of this provision is clearly directed towards the state and not other private parties. Here civil law might be useful in cases where it is possible to prove an actual loss which is directly caused by running the service. It is very unlikely that this will be possible to prove, for example for a shop-owner who says one specific client did not buy one specific item because of bad ratings. Devaluation of buildings or assets is also hardly covered in these scenarios, since it will be hard to prove that the service is the only reason for the change in the value.

Focusing on natural persons, there is a wide range of remedies available at their disposal if the data collected about them is considered personal (following the logic of the above sub-sec-

93 GDPR Art. 5 par. 1 lit. b; DIR Art. 4 par. 1 lit.b.

94 For some guidance on the issue see Dirk Ehlers and Ulrich Becker (eds), *European Fundamental Rights and Freedoms* (de Gruyter Recht 2007) 385–386; PHPHMC van Kempen, 'Human Rights and Criminal Justice Applied to Legal Persons. Protection and Liability of Private and Public Juristic Entities under the ICCPR, ECHR, ACHR and AfChHPR' (2010) 14 Electronic Journal of Comparative Law 1, 29–32.

95 GDPR Recital 14 Sentence 2 states in this regard: "This Regulation does not cover the processing of personal data which concerns legal persons and in particular undertakings established as legal persons, including the name and the form of the legal person and the contact details of the legal person."

tion), although the structure of enforcement might differ for the GDPR and DIR. Leaving general procedural considerations aside and assuming the lawfulness of processing (consent has been given, there is legitimate reason for the collection and processing, etc.)[96], the relevant rights of the data subject are: Knowledge about the information processed or held[97], right of access[98], and the right of rectification and/or erasure[99]. The GDPR contains furthermore a 'right to be forgotten'[100], a right to restrict the processing[101], and a right to object data processing in cases of automated decision making (for profiling or credit scoring for example)[102].

Most of these remedies, like the right to know which data is processed or the rights to alter (have the actual situation reflected in the data) or delete it, are not innovative and stem from times when concerns about data processing related mainly to government use of data.

When it comes to the seemingly more innovative and broadly discussed "right to be forgotten," it should be considered in detail what it actually entails. While one might derive from the actual wording of Art 17 GDPR that an individual is entitled to have a specific piece of personal data deleted completely and everywhere[103], the current situation is more complex. One needs to differentiate a "right to delist" information from the index of a search engine according to the *Google Spain* judgment of the CJEU[104] and a right which is best understood as a more complete right to erasure enshrined in Art. 17 par. 2 GDPR[105]. In summary, while the term "right to be forgotten" suggests protection of data subjects in hindsight, for example when they become identifiable against their will through one of the apps or services that was presented above or while suffering other negative consequences, the actual legal remedies do not hold up to this expectation.

Based on the quality and quantity of legal tools available, it seems that a natural person is fairly protected against the negative consequences of services such as those described in section II, particularly if the party responsible for processing or controlling the data is a private entity. This protection as described in legal texts, however, can sometimes be extremely difficult to ensure in real world scenarios[106].

96 GDPR Art. 6, DIR Art. 8.

97 GDPR Art. 14, DIR Art.13.

98 GDPR Art. 15, DIR Art. 14.

99 GDPR Art. 16, 17, DIR Art. 16.

100 GDPR Art. 17.

101 GDPR Art. 18.

102 GDPR Art. 21.

103 Oskar Josef Gstrein, *Das Recht auf Vergessenwerden als Menschenrecht: Hat Menschenwürde im Informationszeitalter Zukunft?* (Nomos 2016) 198–200.

104 Case C–131/12 *Google Spain* EU:C:2014:317.

105 Oskar Josef Gstrein, 'The Right to Be Forgotten in the General Data Protection Regulation and the Aftermath of the "Google Spain" judgment (C–131/12)' (2017) 5 Privacy in Germany, Datenschutz und Compliance 9, 11–15.

106 Clive Norris and others (eds), *The Unaccountable State of Surveillance: Exercising Access Rights in Europe* (Springer 2016); Robert Rothmann, 'Video Surveillance and the Right of Access: The Empirical Proof of Panoptical Asymmetries' (2017) 15 Surveillance & Society 222.

If the party controlling the data is a competent authority working on public security — e.g. a police force or a city council — the remedies seem to be more limited in quantity. However, this is also a field where procedural safeguards might be applicable that are part of (more nationally diverse) administrative or criminal law. Hence, it is difficult to come to a conclusion which suggests that the protection of an individual is more limited in such scenarios in the EU in general.

Groups

Although the remedies presented above might, at least in theory, provide a fair level of protection against negative consequences for individuals, many of the negative effects outlined in the previous section do not, or not necessarily, occur at the individual level. The reification of prejudices about certain areas for instance does not target any specific individual, and no personal data needs to be included in any part of the analytic procedures leading up to it. The communities — composed of individual, natural persons — living in those areas will be on the receiving end of the negative consequences such as increased police surveillance.

This points to a further potential problem with the definition of personal data in the GDPR and the DIR: it does not cover data which identifies groups of individuals (either formally recognized as a legal person or not), rather than single natural persons. However, the data from apps such as those described above will often refer to specific spots, streets, or neighbourhoods, and consequently the communities living there. If such descriptions don't identify anyone — and why would they? — the entire data protection framework is not applicable.

This is not unique to the case study at hand, but fits into a larger emerging problem area within data protection and privacy legislation in the context of big data analytics. Such analyses are interested in the individual mostly as a member of (myriad) groups, many of which are created by the analyses themselves, unstable in membership and not self-aware[107]. Even if we were to accept that groups should be able to defend their data protection and privacy rights, the question remains how such rights might be protected, especially without negatively impacting the already established level of individual protection[108]. The preventive solutions we discuss in the next sub-section might provide some relief in this regard as well[109].

Potential Preventive Measures on the Basis of the New EU Legislation

The remedies presented so far are exactly that: remedies for when negative consequences have already materialized. When looking at the previous section, however, this does not provide a satisfactory solution for all potential harms: e.g. increased traceability and a generalized loss

107 Linnet Taylor, Bart van der Sloot and Luciano Floridi, 'Conclusion: What Do We Know About Group Privacy?' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy* (Springer 2017) 227.

108 Ugo Pagallo, 'The Group, the Private, and the Individual: A New Level of Data Protection?' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of data technologies* (Springer 2017) 167.

109 Alessandro Mantelero, 'From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era' in Linnet Taylor, Luciano Floridi and Bart van der Sloot (eds), *Group Privacy: New Challenges of data technologies* (Springer 2017) 150–154.

of privacy in public cannot be retro-actively repaired. Interestingly, with the introduction of the GDPR two possibly preventive measures have also been introduced: data protection by design and data protection impact assessments. Article 25 requires data controllers to "implement appropriate technical and organisational measures […] which are designed to implement data-protection principles […] in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects." [110] Furthermore, article 35 of the GDPR requires a data protection impact assessment when "a high risk to the rights and freedoms of natural persons" are foreseen[111].

In the context of the apps discussed, technical measures could for instance include strong and properly implemented encryption where feasible[112]. Also, human–computer interaction design measures could help users to meaningfully exercise their right to be forgotten in the contexts within which the apps are being used[113]. For now, it remains to be seen though how these articles can be given meaning beyond their good intentions, and how to deal with cases in which system developers do not follow preventive guidelines. Although the GDPR does provide for administrative fines of up to ten million Euros or 2% of annual global turnover if article 25 (on data protection by design) has been infringed[114], specific tests still need to be developed in order to be able to adjudicate exactly when this will be the case. Furthermore, it seems unlikely that companies will spontaneously share their design and development processes with outside scrutinizers.

CONCLUSION

As the legal analysis in the above section revealed, the potential problems stemming from services that document fear and reveal "dangerous" areas lie not in the remedies which are legally available within the EU. This seems true, at least, if the data produced is considered to be personal data.

However, this leaves the consideration aside that such remedies must be easy to use for the persons concerned and must be effective. The lessons learned from cases such as *Maximilian Schrems v Data Protection Commissioner*[115] on the Safe Harbor or *Google Spain v AEPD and Mario Costeja Gonzalez*[116] on the "right to be forgotten" seem to suggest that the practical application of rights needs to be facilitated significantly. Furthermore, the interpretation of the jurisprudence in the *Google Spain* case raises three key concerns: in the administration of re-

110 GDPR Art. 25 par. 1.

111 GDPR Art. 35.

112 As proposed by a group of researchers at the Berkman Klein Center of Harvard University: Mat Ollsen, Bruce Schneier and Jonathan Zittrain, 'Dont Panic, Making Progress on the "Going Dark" Debate' (2016) <https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf> accessed 24 March 2017.

113 Lachlan Urquhart and Tom Rodden, 'New Directions in Information Technology Law: Learning from Human–computer Interaction' [2017] International Review of Law, Computers & Technology 1, 6–9.

114 GDPR Art. 83 par. 4 lit. a.

115 Case C–362/14 *Schrems* EU:C:2015:650.

116 Case C–131/12 *Google Spain* EU:C:2014:317. See also Norris and others (n 106) and Rothmann (n 106).

quests, the transparency of decision making processes, and the geographical scope of the right. Nevertheless, at least the setup of the framework seems to be appropriate to tackle the challenges.

A lack of safeguards and remedies results from possible gaps of the definition of "personal data" in texts such as GDPR or DIR. There is a risk that several sources of data will be combined and make individual persons identifiable, even if none of the sources is considered to be personal data itself, e.g. because it only contains certain pieces of information or has been pseudo- or anonymized using state of the art technology. It should be carefully investigated whether such a "release-and-complete-freedom" model[117] is appropriate in regard to datasets which contain information about, for instance, neighbourhoods.

Caution with respect to the release of anonymized data is warranted as it seems unlikely that personal data which has once been de-identified with state of the art technologies will remain risk-free forever. There are incidents which suggest increased caution and consideration: In Australia, a dataset containing seemingly de-identified health records of patients was successfully re-connected with the persons concerned after being published by the government delivering on its commitment to "open data". Even though the government reacted and promptly removed the dataset after notification, it is not unlikely such data will end up on some vending platform in the "darknet"[118]. Highly sensitive data will always contain a certain risk and the question should not be whether the risk can be removed forever and in all circumstances, but rather how it should be managed each and every time the data is being put to use. Possibly, the tendency to publish data aggressively should be countered with a legal requirement that foresees a privacy impact assessment each time the purpose of data processing changes. The UN Special Rapporteur on the right to privacy has also included this topic as one of his main areas of concern for upcoming reports[119].

Furthermore, data about groups of people and local communities is also not covered by the current legal framework. The importance and aspects of group privacy and spaces to develop freely must be studied further in that regard. It is increasingly visible that the deployment of high-tech infrastructure needed to operate "smart cities" or to guarantee increased safety in public through the use of technologies such as CCTV comes with the consequence that spaces for free development of ideas and movements disappear.

The authors would like to coin the term "technological gentrification" in this context. It

117 Sophie Stalla-Bourdillon and Alison Knight, 'Anonymous Data v. Personal Data—a False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data' (2016) 34 Wisconsin International Law Journal 284, 322.

118 Paul Farrell, 'The Medicare machine: patient details of 'any Australian' for sale on darknet' (The Guardian, 03 July 2017). <https://www.theguardian.com/australia-news/2017/jul/04/the-medicare-machine-patient-details-of-any-australian-for-sale-on-darknet> accessed 29 August 2017.

119 The report on dangers of Big Data & Open Data is expected to be presented to the General Assembly in 2017. United Nations, Office of the High Commissioner of Human Rights, 'Planned Thematic Reports and call for consultations' < http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx> accessed 29 August 2017.

describes the slow-down (and perhaps ultimate death) of societal development as a result of the endeavour to provide increased security and predictability in public spaces as a consequence of the inappropriate mass use of invasive technologies such as (smart) CCTV or mobile devices as stigmatizing security sensors. The chilling effects resulting from this situation — the permanent observation of public behaviour — set the stage for a world of continuous ex-ante compliance. This means that certain areas of cities or entire communities will lose their potential to re-develop by experimenting with new forms of societal interaction.

There is a growing and interesting body of literature in this context on the development of smart cities and the impact of technologies like CCTV[120]. However, it remains questionable whether such mostly theoretical knowledge will see a sufficient transfer to the broader ranks of society which are subjected to highly sophisticated technologies without being completely aware of its basic functioning and the consequences of its use.

It is important to remember at this stage that secondary law, such as the GDPR and the DIR, is based on primary EU law such as the CFEU. The wording of Art. 8 CFEU and the fact that it is a right different from Respect for private and family life (Art. 7 CFEU) suggests that in the EU the term "personal data" has to be interpreted broadly since it is not necessarily tied to the context of the use of data or traditional privacy rights[121]. Hence, it might perhaps be possible to interpret the definition of personal data to include datasets that are the result of apps and services such as those discussed in this article.

At the moment though, it seems that the EU legal framework alone will not suffice as a solution for all the potential problems presented. What is thus clear is that — especially because it remains largely an open matter how services which describe neighbourhoods or deal with the perception of fear may impact certain areas and people — various issues will deserve continuing scrutiny in order to hopefully be able to develop workable solutions to emerging problems early on.

First, the legal analysis has focused solely on EU data protection framework. Nevertheless, the legal context with regards to privacy, data protection and informational self-determination

120 For a comprehensive overview on topics relating to Smart Cities see Houbing Song, Ravi Srvinivasan, Tamim Sookoor and Sabina Jeschke (eds), *Smart cities: Foundations, Principles, and Applications* (John Wiley & Sons 2017). For CCTV see Demetrius Klitou, 'Public Space CCTV Microphones and Loudspeakers: The Ears and Mouth of "Big Brother"' in Demetrius Klitou*, Privacy Invading Technologies and Privacy by Design* (Springer 2014) 114, 116.

121 Art. 8 CFEU, Protection of Personal Data, states in par. 1: "Everyone has the right to the protection of personal data concerning him or her." This also would support the argument by the CJEU that Art 8 is a different fundamental right than Art. 7 CFEU on Privacy, as stated prominently in Joined Cases C–203/15 and C–698/15 *Tele2 Sverige* EU:C:2016:970, para 129, last sentence. The question arises because the jurisprudence of the European Court of Human Rights seems currently, at least for practical purposes, equivalent in terms of the scope of protection applicants are being granted. Note here also that Art. 8 of the European Convention on Human Rights is very similar to Art. 7 CFEU. Additionally, Art. 53 CFEU guarantees that the level of protection offered is at least equivalent to the European Convention on Human Rights and ties the substantial privacy protection of both treaties even closer. Hence, the question remains what the added value of Art 8 CFEU would be. Although the added value might not be apparent at this point in time, it might become clearer in the future as a result of technological developments and changing uses of personal data.

diverges widely around the world and it is being discussed whether these rights are the same or different[122]. The concerns and apps discussed, however, do not neatly follow jurisdictional lines. Most apps are available for download by interested users in repositories such as the Google Play store and the Apple app store without geographic restrictions; and where they are targeted at specific issues in specific locations — such as the Free to be app in Melbourne — copies for other locations can be produced at relatively low economic costs. The authors hope to have sketched out some legal challenges and ways forward which will also be applicable in other jurisdictional contexts, but much work clearly remains in this regard.

Second, such systems might become the basis for "evidence based" prejudices and discrimination. Data in itself can only suggest certain conclusions, even if it is already analysed and processed using complex algorithms and substantive computing power. Humans must understand the criteria on which such suggestions are based and not look at them naively, or worse, base decisions on them which might negatively impact individuals.

Third, terms like "safe," "unsafe," "good," and "bad" are very difficult to rate on simple scales. A neighbourhood that is stimulating and interesting for one person might be scary and terrifying for another. Breaking down such notions in quantifiable categories leads to a loss of descriptive richness. This problem is amplified when the judgments or impressions of a group of people are aggregated to single conclusions. Will reviews of neighbourhoods indeed impact dwellers, real estate owners, and local businesses in the way user generated reviews can drive restaurants out of business[123]? And what will the potential for abuse of such services be if certain individuals find ways to discredit areas through fake reviews or reports?

Finally, and connected to the previous issue, yet another techno–social system has been added to the surveillance assemblage operating in the urban environments. It contributes to a pervasive remaking of how we experience privacy in public spaces, and curtails the free development of personalities and communities. With some modifications, many of the problems and solutions discussed in this paper might be applicable to many similar systems which (enable users to) track, log, trace, analyse, and rate whatever takes place in public. The question arises when enough is enough: which technology is the straw that breaks the camel's back?

122 For example, the UN Special Rapporteur on the right to privacy has launched a conference series with the title "Privacy, Personality and Flows of Information" which is envisaged to result in a report on the subject in October 2020. For more information visit <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx> accessed 18 August 2017.

123 Michael Luca, 'Reviews, Reputation, and Revenue: The Case of Yelp.com' [2016] Harvard Business School working paper 12-016.